Betacom

Securing Private Networks

Executive Summary

Enterprises require secure data networks that can be trusted with business-critical tasks, especially for Industrial IoT applications, and they are increasingly interested in owning their own wireless networks to maintain control over their data and network performance. Security has become a key consideration as enterprises start to evaluate private wireless networks as a high performance option for managing essential business applications and operations. What are the factors that make a private 4G/5G network more secure than a Wi-Fi network? What are the advantages of a private network over a public network? What factors should be explored in evaluating the differences between private network solutions on the market?

This paper highlights the 5G security features that form the foundation of secure private networks. It then details the additional security benefits that a well planned, well managed private network can offer enterprises to ensure that their private network and their data is secure.

The Foundation: 5G Security

4G/5G networks have demonstrable security advantages over Wi-Fi networks. Built on global standards that have been hardened for years, 4G networks use SIMs and multifactor authentication to help ensure authorized access to the network. 5G adds new protections at the device, radio and core network layers to authenticate and isolate devices, making it possible to securely deploy a wide range of machines, robots and sensors to enable Industry 4.0 use cases:

Figure 1: 5G Security Controls

A private 5G network offers superior security due to the strong authorization, authentication and access control features summarized in Figure 1. In particular:

- The 5G network uses **data encryption** and **integrity protection mechanisms** to protect the data transmitted by the enterprise, prevent information leakage, and enhance data security. Both **signaling plane and user plane traffic is encrypted**, leveraging the strong and well-proven security algorithms from 4G.
- Adoption of **Software-Defined Network (SDN)/Network Function Virtualisation (NFV)** in the architecture of 5G systems facilitates the **virtualisation of traditional security functions like firewalls, access authentication, SSL**, etc. These services can be deployed with increased flexibility, providing improved security.
- 5G introduces a new network architecture element, the **Security Edge Protection Proxy** (SEPP). The SEPP **protects the enterprise network edge, acting as the security gateway** on interconnections between the private enterprise network and outside networks to prevent tampering or eavesdropping.
- Use of **Edge Computing** supports the ability to localise and isolate data traffic allowing information to be kept entirely within the customer premises for complete control of data flow within the enterprise without dependency on external elements for communication. It is also possible to localise and isolate the 'control plane' from the 'user plane' for enhanced protection from external attacks.

- For **time critical applications** the 5G private network can be transparently integrated into one or more **'Time Sensitive Network'** bridges to safeguard time-sensitive communications from network attacks. This ensures correct ongoing operation of both the 5G network and time critical industrial devices and applications particularly benefiting use cases requiring 5G Ultra-Low Latency and Reliable Communications.
- A new **authentication framework** is introduced with 5G which allows the enterprise to provide secure 'plug-in' device authentication procedures. Importantly, this enables an enterprise to manage identity and access from its own protected IT systems.
- Proven **SIM/eSIM technologies can be also used for authentication, authorization and access control,** efficiently offering higher security than typical approaches using Wi-Fi keys or MAC address controls.
- Improved **protection of device identity 'over-the-air'** including protection against false base stations. 5G networks use a combination of 'SUPI', a Subscription Permanent Identifier, and 'SUCI' a Subscription Concealed Identity to manage identity of devices. This combination provides **privacy preserving protection of device and user identity**, ensuring that the true identity cannot be stolen. This control also prohibits moving a 5G SIM from one device to another without changing security keys.
- Network management can be decoupled so that the enterprise can outsource infrastructure management to a **managed service provider** who can apply their **world class knowledge in monitoring and maintaining security** to the private network.

The Betacom 5G as a Service Security Advantage

Betacom 5G as a Service (5GaaS) is a 4G/5G private wireless solution provided as an end-to-end managed service from wireless service experts. It deploys rapidly and delivers high reliability, cost effectiveness, enterprise security, superior bandwidth, and low latency. Betacom 5GaaS sits behind the enterprise's firewall to connect business-critical devices and applications including IoT devices, laptops, cameras, robots, signage, machinery, and virtual reality applications. The solution leverages the best of 4G and 5G technologies to gain optimal value and performance for each customer's target business applications.

Betacom 5GaaS is a managed service. This means that we plan, design, install and operate the network, while providing the enterprise with visibility into network performance. We have built security into every element of our service with a Zero Trust design principle. We manage the network from a modern Security and Service Operations Center (SSOC). The SSOC is enabled with cloud-based applications that use artificial intelligence and machine learning to proactively monitor the network and respond to threats in real time. Betacom 5GaaS is based on 4G/5G standards, using both SIMs and multifactor authentication to ensure that only authorized devices are allowed onto the enterprise private wireless network. All network components can be deployed behind the enterprise firewall, and traffic is separated so that Enteprise data stays inside your business. The control plane data we use to monitor and manage the network is encrypted end-to-end, adding additional security without impacting network performance or bandwidth.

Betacom 5G-as-a-Service E2E Security

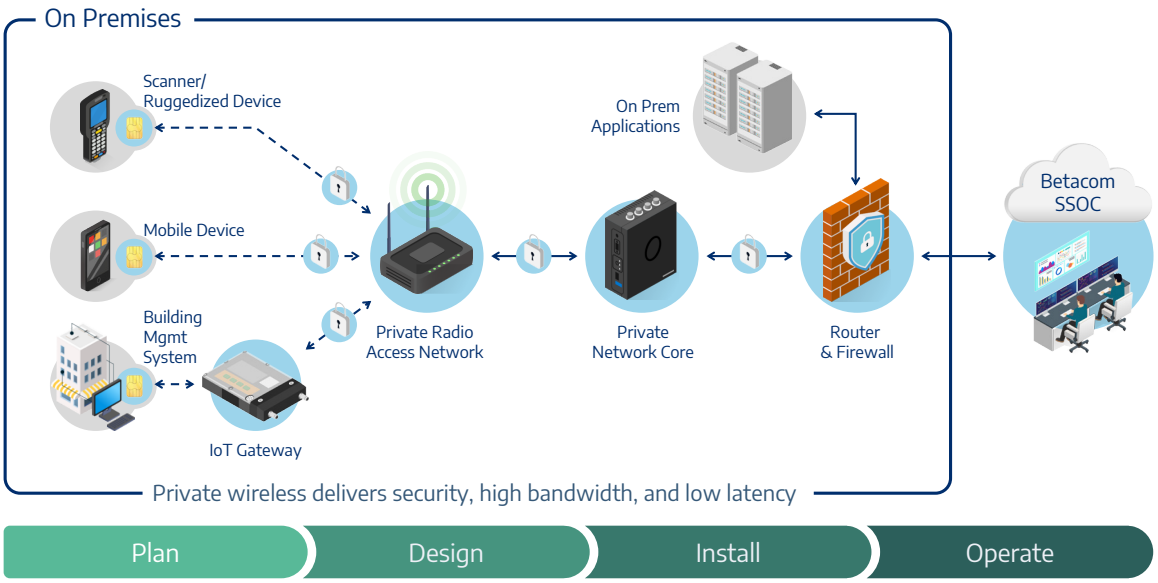

Figure 2: Betacom 5GaaS Architecture

Here are some of the key security elements that we've designed into each phase of service delivery to ensure end-to-end solution security:

Plan

Security starts in planning stage. Along with establishing the detailed technical and performance requirements and establishing the applications that will run on the network, we work with our customers to establish the security and policy principles for the network. We meet with your IT team to understand how our private wireless infrastructure will interconnect with the existing LAN/WAN infrastructure and how to best deploy the private wireless network to reach back-end application systems and interconnect with our SSOC. This ensures that we understand the enterprise business, security concerns, and network and security systems in place so that we can design appropriately and execute against specific requirements.

Design

During the design phase we establish the network architecture. This includes laying out the nodes that will be accessing your network, and what devices will be accessing these nodes and from where. We take into account your existing firewall and help make informed decisions about additional security measures that might be needed. The deliverables from this phase include the location of all required private wireless equipment (private radio access network, private wireless core and security gateways), an RF design that shows a heat map of coverage, a full bill of materials (BOM), and mutual decisions about where the network will reside.

Install

Before we step foot on a new installation site we stage the private network in order to harden the security of each element in 5GaaS. We then install the system behind the enterprise firewall, ensuring that each network element is connected over a secure channel. Our highly trained installation crews have in-depth expertise in deploying 4G/5G networks, limiting risk associated with deployments. Our teams are focused on understanding precise requirements and troubleshooting needs with risk avoidance strategies to keep projects on track and within budget. In addition to performance tests, we will run security tests to ensure the network is running as designed.

Operate

Once we've installed the Betacom 5GaaS network, our managed service value begins as we proactively monitor the network 24x7 from our SSOC. We leverage Artificial Intelligence/Machine Learning (AI/ML) based applications to detect system anomalies, alerts or alarms. Our SSOC then proactively assesses and guides response actions to ensure a continuously available service using AI backed up by U.S.-based Engineers. The AIOps system continuously improves as new threat behavior is detected and new rules are created. Enterprises have dashboard access into network performance for additional assurance that the private wireless network is performing as specified. We run periodic vulnerability scans to ensure the setup continues to be protected and has the latest updates. Our SSOC technical support team is also available 24x7 to address issues.

A Word About Our Security Partnerships

We have partnered with cybersecurity experts to harden all security aspects of Betacom 5GaaS. From next generation firewalls to up-to-date threat analysis, best-in-class security technology is built into our solution to continuously assesses risks and automatically adjusts to provide comprehensive real-time protection across the digital attack surface. The combination of Betacom 4G/5G and security expertise with industry leading security tools ensures that our enterprise customers are deploying the latest technology that reduces risk while providing a platform for business growth through private cellular wireless operational efficiency and automation.

Conclusion

Private wireless networks offer enterprises a new connectivity option for business-critical applications that require reliable high-speed, low latency performance. Betacom 5GaaS is founded on 4G/5G standards and is managed through our Security and Service Operations Center with the latest in AIOps and cybersecurity management to give our customers the peace of mind that all elements of security have been designed into the solution with zero trust principles. Security is not an afterthought. It drives every element of our managed private network service.